

Remarks

Applicant thanks the Examiner for signing the references cited in the IDS submitted. The Official Action rejected claims 1-4, 7, 9-12, 15, 17-20, 23-31, and 33 and objected to claims 5-6, 8, 13-14, 16, 21-22, and 32. Claims 1, 9, 17, 23, 27, 32, and 33 have been amended and claim 31 has been canceled. Claims 34-36 have been added. Claims 1-30 and 32-36 are now pending in the present application. Applicant respectfully requests reconsideration and allowance of the pending claims in the light of the points that follow.

Allowable Subject Matter

Applicant gratefully acknowledges that claims 5-6, 8, 13-14, 16, 21-22, and 32 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicant has rewritten claim 32 in independent form including all of the limitations of the base claim and any intervening claims. Applicant's intention is to merely place claims 32 in independent form and not to narrow the scope of such claim beyond the scope as originally filed. Applicant, however, has elected not to rewrite such claims 5-6, 8, 13-14, 16, 21-22 at this time since Applicant believes the claims from which they depend are also allowable.

Claim Rejections – 35 USC § 102

The Official Action rejected claims 1-4, 7, 9-12, 15, 17-20, 23-31, and 33 under 35 USC 102(b) as being anticipated by Weixin et al ("A systolic Linear Array for Modular Multiplication"). Applicant has amended claims 1, 9, 17, 23, 27, 32, and 33 and has

canceled claim 31. Applicant respectfully requests the rejection of claims 1-4, 7, 9-12, 15, 17-20, 23-30, and 33 be withdrawn.

As is well-established, in order to successfully assert a *prima facie* case of anticipation, the Official Action must provide a single prior art document that includes every element and limitation of the claim or claims being rejected. Therefore, if even one element or limitation is missing from the cited document, the Official Action has not succeeded in making a *prima facie* case.

Each of claims 1, 9, 17, 23, and 27 comprise a modular multiplier including a plurality of independent channels, wherein the plurality of independent channels include a first computation channel and a second computation channel **each capable of performing an independent modular multiplication operation**. The Official Action appears to rely on Fig. 2-4 for teaching of independent channels each capable of performing an independent modular multiplication operation. Applicant respectfully points out that Fig. 2 discloses merely a single modular multiplier comprising 4 processing elements (PE) processing inputs such as c_{in} , q_{in} , and b_{in} for performing a single modular multiplication operation as described in right column, lines 1-14 of page 173. Inputs c_{in} , q_{in} , and b_{in} respectively represent carry from lower significant bits to higher significant bits, least significant bits of the partial product terms, and bits of a multiplicand. Each PE may process the corresponding inputs to perform a single modular multiplication by a shift-and-add approach. Thus, Weixin only appears to teach a plurality of processing elements that perform a single multiplication operation based upon inputs c_{in} , q_{in} , and b_{in} and does not teach a modular multiplier comprising independent computation channels **each capable of performing an independent modular multiplication operation** as required by claims 1, 9, 17, 23, and 27.

Claims 2-8 and 34, 10-16 and 35, 18-22 and 36, 24-26, and 28-30 depend respectively on claims 1, 9, 17, 23, and 27. Therefore, claims 2-8 and 34, 10-16 and 35, 18-22 and 36, 24-26, and 28-30 are at least allowable for the reasons noted above in regard to claims 1, 9, 17, 23, and 27. Further, claim 33, as amended, depends from claim 32 which the Examiner indicated was allowable. Accordingly, claim 33 is also allowable. Applicant respectfully requests the rejection of claims 2-8 and 34, 10-16 and 35, 18-22 and 36, 24-26, 28-30, and 33, 1, 9, 17, 23, 27, and 32 be withdrawn.

If the Examiner elects to maintain the present rejection of claims 1-4, 7, 9-12, 15, 17-20, 23-31, and 33, Applicant respectfully requests the Examiner to identify with more specificity (e.g. column and line number) where Weixin teaches a modular multiplier including a plurality of independent channels each performing an independent modular multiplication operation. Allowance of claims 1-4, 7, 9-12, 15, 17-20, 23-30, and 33 is respectfully requested.

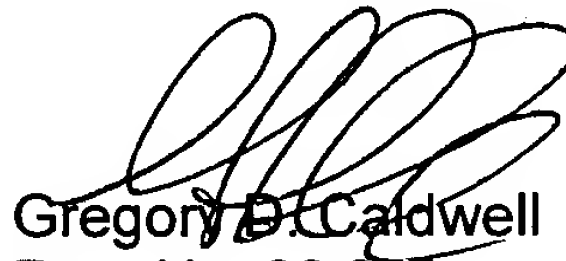
Newly Added Claims

Newly added claims 34-36 each depend from one of claims 1, 9 and 17. Accordingly, each of claims 34-36 is allowable for at least the reasons stated above in regard to claims 1, 9 and 17. Further, each of claims 34-36 include additional limitations that are not taught or suggested by the cited art. In particular, each of claims 34-36 require a first computation channel and a second computation channel that operate as two modular multipliers in a first mode of operation and as a single modular multiplier in a second mode of operation. Allowance of claims 34-36 is respectfully requested.

Conclusion

The foregoing is submitted as a full and complete response to the Official Action. Applicant submits that the application is in condition for allowance. Reconsideration is requested, and allowance of the pending claims is earnestly solicited. Should it be determined that an additional fee is due under 37 CFR §§1.16 or 1.17, or any excess fee has been received, please charge that fee or credit the amount of overcharge to deposit account number 02-2666. If the Examiner believes that there are any informalities, which can be corrected by an Examiner's amendment, a telephone call to the undersigned at (503) 439-8778 is respectfully solicited.

Respectfully submitted,


Gregory D. Caldwell
Reg. No. 39,926

c/o Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1030
408-720-8300

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL WITH SUFFICIENT POSTAGE IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313

ON: 10/29/04
Date of Deposit

NAME OF PERSON MAILING CORRESPONDENCE

Richard Brown

Signature R. Brown